What Is Claimed Is:

1. A method for verifying a digital signature used for verifying a digital signature of a message, wherein

a digital signature issue side apparatus performs:

a signature issuing step comprising applying a secret key owned by a digital signature issuer to the message or a hash value of the message to issue a digital signature on the message, and

a registration step comprising delivering the message with digital signature including the issued digital signature and message and registering log data of the message with digital signature in a log list, and

a digital signature verifier side apparatus performs:

a verification target acceptance step comprising accepting the delivered message with a digital signature as a message with a verification target digital signature,

a history acquisition step comprising acquiring a log list of the digital signature issuer who has delivered the message with a verification target digital signature, and

a history existence verification step comprising checking whether or not log data of the message with a verification target digital signature is registered in the log list , and

if a check result is YES, the method additionally comprises:

an individual reliability setting step comprising the reliability of the log data included in the log list ,

a history reliability calculation step comprising calculating reliability of the log list based on the set individual reliability, and

a verification step comprising authenticating a fact that the message with a verification target digital signature is delivered from the digital signature issuer side apparatus .

2. An apparatus for verifying a digital signature comprising:

verification target acceptance means for accepting a message with a verification target digital signature,

history acquisition means for acquiring a log list of the digital signature issuer who has delivered the message with a verification target digital signature,

history existence verification means for checking whether or not log data of the message with a verification target digital signature is registered in the log list,

individual reliability setting means for setting reliability of the log data included in the log data if the log data of the message with a verification target digital signature is registered,

history reliability calculation means for calculating reliability of the log list based on the set individual reliability, and

verification means for authenticating with reliability a fact that the message with a verification target digital signature is delivered from the digital signature issue side apparatus.

3. A method for arbitration used for solving a dispute on a digital signature of a message, wherein the method for arbitration comprises:

a request acceptance step comprising accepting a message with an arbitration target digital signature from an arbitration requestor apparatus,

acquiring a log list of the message with an arbitration target digital signature ,

verifying a fact that the message with a digital signature that has been requested for verification has been issued by a digital signature issue side apparatus by use of the acquired log list of the digital signer, and

an arbitration step comprising outputting an arbitration result is output based on reliability that is an output in the verification step.

4. An arbitrator apparatus for solving a dispute on a digital signature of a message comprising:

request acceptance means for accepting a message with an arbitration target digital signature,

history acquisition means for acquiring a log list of the message with an arbitration target digital signature,

history existence verification means for checking whether or not the log data of the message with an arbitration target digital signature is registered in the log list,

individual reliability setting means for setting the reliability of the log data included in the log data if the log data of the message with an arbitration target digital signature is registered,

history reliability calculation means for calculating reliability of the log list based on the set individual reliability, and

arbitration means for outputting an arbitration result based on the reliability.

5. A method for managing the log list, which is a issuing history of a digital signature issued on a message by a digital signature issue side apparatus, in a log list storage side apparatus comprising:

accepting the log list from the digital signature issue side apparatus,

verifying validity of the digital signature of the digital signer signed on the log list or log list registration request data,

verifying consistency between the accepted log list and a registered log list of the registered digital signer, and

adding and registering the log list with the confirmed consistency to the registered log list of the digital signer.

6. The method for managing a log list according to claim 5, further comprising:

confirming the consistency is confirmed, and

transmitting a fact that the log list is added and registered to the registered log list of the digital signer, to a digital signer side apparatus.

7. A method for managing a log list according to claim 5 comprising:

a step in which the digital signature issue side apparatus requests registration of the log list to the log list storage side apparatus, and

a step in which log data other than the newest log data included in the log list is deleted if the additional registration notice is received.

8. The method for verification of a digital signature according to claim 7, wherein

the digital signature issue side apparatus performs:

a step comprising issuing electronic data of a deposition request document for indicating intention of a registration request , and

a step comprising transmitting the issued deposition request document electronic data, a public key certificate, and log list data, to the log list storage side apparatus, and

as the step for verifying the validity of the digital signature, the log list storage side apparatus performs:

a step comprising verifying the validity of the received public key certificate , and

a step comprising checking whether or not the deposition request document is verified correctly by use of the public key of the user included in the public key certificate .

9. The method for verifying a digital signature according to claim 7, wherein the digital signature issue side apparatus requests registration of the log list every time when a digital signature is issued.

10. A method for verifying a digital signature in which a log list storage side apparatus verifies a digital signature that a digital signature issue side apparatus has issued on a message, wherein the digital signature apparatus performs:

a signature issuing step comprising applying a secret key owned by the digital signature issue to the message or a hash value of the message, to issue a digital signature on the message,

a registration step comprising registering log data of the message with a digital signature in a log list, and

requesting registration of the log list to the log list storage side apparatus,

the log list storage side apparatus performs steps including:

accepting the log list registration request from the digital signature issue side apparatus,

verifying validity of the digital signature issued by the digital signer signed on the log list or the log list registration request included in the log list registration request ,

verifying consistency between the accepted log list and a log list of the digital signer that has already been registered ,

accepting a verification request of the message with a digital signature from the external, and

authenticating a fact that the message with a digital signature that has been requested for the verification has been issued by the digital signature issue side apparatus, by use of the registered log list of the digital signer.

11. The method for verification according to claim 10 wherein:

the digital signature issue side apparatus performs steps further including:

transmitting the issued digital signature and the message with a digital signature including the message to the digital signature receiver side apparatus, and

the digital signature receiver side apparatus performs steps further including:

receiving the message with a digital signature , and

requesting verification vicarious execution of the message with a digital signature to the log list storage side apparatus, and

the log list storage side apparatus performs steps further including:

accepting the verification request of the message with a digital signature that the digital signature receiver side

apparatus has received from the digital signature issue side apparatus from the digital signature receiver side apparatus.

12. The method for verification according to claim 10, wherein the log list storage side apparatus registers the digital signature on the log list after correctness of the digital signature is confirmed in the verification step.

13. The method for verification according to claim 10, wherein the log list storage side apparatus performs steps further including:

receiving a verification vicarious execution request from a verification vicarious execution requestor apparatus, and

transmitting a verification result to the verification vicarious execution requestor apparatus.

14. The method for verification according to claim 10, wherein the log list storage side apparatus accepts the log list registration request from plural digital signature issue side apparatuses.

15. The method for verification according to claim 11, wherein each step carried out in the digital signature receiver side apparatus is carried out in an arbitration requestor apparatus used by an arbitration requestor who requests arbitration of correctness of a signature issued by the signer.

16. A log list storage side apparatus for verifying a digital signature issued in a digital signature issue apparatus comprising:

a memory unit for registering a log list,

reception means for accepting log list registration request from the digital signature issue side apparatus,

means for verifying validity of a digital signature issued by the digital signer signed on the log list or the log list registration request included in the log list registration request,

means for verifying consistency between the accepted log list and a log list of the digital signer registered in the memory unit,

verification means for authenticating a fact that the message with a digital signature that has been requested for the verification vicarious execution has been issued by the digital signature issue side apparatus by use of the registered log list of the digital signer registered in the memory unit, and

transmission means for transmitting a verification result to the external.

17. The method for arbitration according to claim 3, wherein the method further comprises:

requesting the log list from a management apparatus that manages a log list of a message with an arbitration target digital signature , and

acquiring the log list of the message with an arbitration target digital signature from the management apparatus.

18. The log list storage side apparatus according to claim 16, wherein the memory unit registers the digital signature having consistency that has been confirmed by the verification means to the log list additionally therein.

19. The log list storage side apparatus according to claim 16, wherein:

the reception means accept a verification vicarious execution request of the received message with a digital signature from the digital signature receiver side apparatus that has received the digital signature issued and transmitted by the digital signature issue side apparatus, and

the transmission means transmit a verification result to the digital signature receiver side apparatus.